Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report
for 20 November 2003

Daily Overview

- Dow Jones Business News reports the U.S.–Canadian investigative task force says FirstEnergy Corp.'s failure to monitor its network of power lines and react to problems was largely responsible for North America's largest blackout on August 14. (See item 3)

- The San Diego Union–Tribune reports prosecutors have announced that they have broken up a sophisticated identity–theft ring that preyed on victims across San Diego County, CA. (See item 7)

- ABC News reports a suspected arson fire is disrupting train travel up and down California. (See item 10)

DHS/IAIP Update *Fast Jump*

Production Industries: **Energy**; **Chemical**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information and Telecommunications**; **Internet Alert Dashboard**

Other: **General**; **DHS/IAIP Web Information**

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – http://esisac.com]

1. *November 19, Reuters* — **Storm cuts power to 35,000 in Washington state. Strong winds that toppled trees and sheared power lines in Washington state on Wednesday, November 19, cut electricity service to about 35,000 homes and businesses, local utilities reported. The Spokane, WA, area suffered the biggest blow, with winds of 50 miles per hour leaving 20,000 customers of Avista Corp. without power.** "We have a lot of trees and lines down and a lot of individual service problems," Avista spokesperson Debbie Simock said by telephone.

Across the state in western Washington, some 15,000 customers were in the dark, including 5,000 served by Seattle City Light, another 5,000 customers of Puget Sound Energy, and 4,000 in the Snohomish County Public Utilities District.
Source: http://biz.yahoo.com/rc/031119/weather_washington_outages_1. html

2. *November 19, Dow Jones Business News* — **EIA to provide regular LNG data next year. Energy Information Administration Chief Guy F. Caruso said his agency will begin providing storage data on liquefied natural gas (LNG) in the U.S. beginning in 2004. Caruso said the agency is now accumulating data for the LNG report,** but did not specify when the data would be released. The agency, the statistical arm of the Department of Energy, now provides monthly and weekly storage data for working natural gas. Caruso said his agency will receive additional monies for staff and other needs in President Bush's 2004 fiscal–year budget.
Source: http://biz.yahoo.com/djus/031119/1504001307_2.html

3. *November 19, Dow Jones Business News* — **Panel puts bulk of blame for August blackout on FirstEnergy. FirstEnergy Corp.'s failure to monitor its network of power lines and react to problems was largely responsible for North America's largest blackout on August 14, said the U.S.–Canadian task force investigating the unprecedented event. In a harsh indictment of the Ohio utility's performance that day, the task force said FirstEnergy's failure to maintain its systems, trim trees and notify its neighbors led to a series of transmission–line outages that precipitated North America's largest blackout and allowed it to spread.** The blackout was "largely preventable," said U.S. Energy Secretary Spencer Abraham. "Once the problem grew to a certain magnitude, nothing could be done to prevent it from cascading." The report found FirstEnergy violated grid–reliability rules set up by the North American Electric Reliability Council, including the utility didn't take the necessary action to return its system to a safe operating state within 30 minutes of losing the Chamberlin–Harding line, and FirstEnergy didn't notify other systems of an impending emergency. The Midwest ISO, the grid monitor for much of the Midwest, also violated the council's rules by failing to notify other reliability coordinators of potential problems, the report said. The Midwest ISO also lacked adequate capability to monitor grid conditions. Report: https://reports.energy.gov/
Source: http://biz.yahoo.com/djus/031119/1500001305_2.html

[Return to top]

Chemical Sector

4. *November 16, CBS 4 Denver* — **60 Minutes special report: U.S. plants open for terrorists.** There are 15,000 facilities across the United States that produce or store deadly chemicals –– chemicals that terrorists could use against us as weapons of mass destruction –– and many have lax security. **The Justice Department calls this threat "real and credible." Yet, two years after September 11, 60 Minutes Correspondent Steve Kroft reports that chemical plants are still not subject to federal regulations when it comes to security.** There are more than 100 chemical plants –– in backyards all across the United States –– where a catastrophic accident or an act of sabotage by terrorists could endanger more than a million people. One plant in Chicago could affect almost three million people. And in California, the chemicals at

one site have the potential to kill, injure or displace more than eight million people. **These statistics have come from the chemical companies themselves. Federal law requires them to file a "risk management plan" with the Environmental Protection Agency, describing the "worst" case scenario that could happen at their plant.** In its investigation visiting dozens of plants in major metropolitan areas, 60 Minutes found among other things, gates unlocked or wide open, dilapidated fences, and unprotected tanks filled with deadly chemicals that are used to manufacture everything from plastics to fertilizer.
Source: http://news4colorado.com/topstories/topstories_story_3201933_54.html

[Return to top]

Defense Industrial Base Sector

5. *November 18, Government Accounting Office* — **GAO−04−253T: Defense Acquisitions: Improvements Needed in Space Systems Acquisition Policy to Optimize Growing Investment in Space (Testimony). The Department of Defense (DoD) is spending nearly $18 billion annually to develop, acquire, and operate satellites and other space−related systems. The majority of satellite programs that the Government Accounting Office (GAO) has reviewed over the past two decades experienced problems that increased costs, delayed schedules, and increased performance risk.** In some cases, capabilities have not been delivered to the warfighter after decades of development. DoD has recently implemented a new acquisition policy, which sets the stage for decision making on individual space programs. GAO was asked to testify on its assessment of the new policy. GAO did not make recommendations in its testimony. However, it reiterated a previous recommendation to modify its policy to separate technology development from product development. DoD disagreed with GAO's earlier recommendation because it believes that the modification would slow down acquisitions, increase risks, and keep DoD from taking advantage of cutting edge technology.
Testimony: http://www.gao.gov/new.items/d04253t.pdf
Source: http://www.gao.gov/highlights/d04253thigh.pdf

[Return to top]

Banking and Finance Sector

6. *November 19, Associated Press* — **Feds accuse 47 currency traders of fraud. Federal authorities announced criminal charges Wednesday, November 19, against 47 currency traders in a nationwide crackdown on alleged fraud in the foreign exchange market. Some of the traders cheated average investors out of funds totaling millions of dollars, while others set up rigged currency transactions to cheat well−known banks in exchange for cash kickbacks, authorities said.** In some of the scams, U.S. Attorney James Comey said, traders said they were from financial institutions with "fancy−sounding names" and gave individuals the false sense they were making safe investments −− then simply stole their money. In another part of the scheme, traders would persuade their banks to engage in rigged trades designed to produce losses for the banks −− then take kickbacks from co−conspirators who made money on the trades, Comey said. Authorities said they had made 37 arrests and filed criminal complaints or indictments against the 47 people.

Source: http://www.washingtonpost.com/wp−dyn/articles/A62101−2003Nov 19.html

7. *November 18, San Diego Union−Tribune (CA)* — **Task force smashes ID−theft ring. Prosecutors announced on Monday, November 17, that they have broken up a sophisticated identity−theft ring that preyed on victims across San Diego County, CA. The ring swindled hundreds of people in the county as well as sailors aboard the aircraft carrier Nimitz, where one of the accused was a crew member, prosecutors said.** Prosecutors described an operation unique because of its assembly−line sophistication. **Some members collected information, primarily by stealing mail, while others manufactured false identification cards and bogus checks, and others cashed the checks, they said.** During secret proceedings over four weeks, a special grand jury heard from 83 victims and indicted 21 defendants on 154 counts of conspiracy, theft, forgery, fraud and other charges October 31. Prosecutors showed grand jurors phony state and military identification cards and forged checks. There was no indication that the false military IDs were used to enter any bases, prosecutor Corinne Miesfeld said. Authorities arrested 10 people during raids a week ago, she said. Other defendants were already in custody or have been arrested since. Four remain at large. Miesfeld said the investigation is continuing and that charges are expected to be filed against more people connected with the ring.
Source: http://www.signonsandiego.com/news/metro/20031118−2218−idthe ft.html

[Return to top]

Transportation Sector

8. *November 19, Government Executive Magazine* — **FAA announces organizational overhaul. The Federal Aviation Administration (FAA) unveiled a major reorganization Tuesday that consolidates offices and management positions and calls for the agency to do a comprehensive analysis to determine if its workforce should be downsized.** Under the plan, the FAA will eliminate current "stovepipe" offices and management positions in favor of new business units and groups, said Russ Chew, who left American Airlines to develop the reform plan as the FAA's first chief operating officer. Among other changes, the plan designates certain FAA executives as vice presidents of the new business units. **The shakeup is intended to make the FAA leaner and more responsive to Congress, the flying public and employees, said the agency's administrator, Marion Blakey. "The FAA is going to be a much more accountable, efficient and performance−based organization," she said.** However, Chew and Blakey said it is too early to know if the plan will result in downsizing. The FAA will spend several months establishing new performance standards for safety, service, cost and productivity, Chew said. The new vice presidents will take the helm of their respective units within two months and then make recommendations on further changes.
Source: http://www.govexec.com/dailyfed/1103/111803c2.htm

9. *November 19, Government Executive Magazine* — **TSA lets airport directors restrict screeners' holiday leave. The Transportation Security Administration (TSA) has issued guidance giving federal security directors at the nation's airports the ability to restrict leave and require overtime for passenger and baggage screeners during the Thanksgiving holiday.** TSA is gearing up for a busier holiday travel season than last year. **The Homeland Security Department is allowing the federal security directors at airports to take a**

number of steps to reduce passenger wait times while maintaining security, said Asa Hutchinson, its undersecretary for border and transportation security, at a news conference Tuesday. Those steps include restricting time off and requiring overtime for screeners, putting managers on the front lines with screeners, and coordinating schedules with airlines to ensure the appropriate number of screeners are in the right locations. TSA is leaving it up to the security directors to decide exactly which steps should be implemented depending on their unique circumstances, said spokesman Brian Turmail.
Source: http://www.govexec.com/dailyfed/1103/111803c1.htm

10. *November 19, ABC30 (Fresno, CA)* — **Possible arson fire interrupts travel.** A suspected arson fire is disrupting train travel up and down California. **It started overnight on a trestle just east of Chowchilla and quickly spread. Investigators don't know how a bridge caught fire, but they suspect it may be part of a string of fires in the area. The rail line is the one of the central pipelines for Northern and Central California.** Right now, Amtrak is having to bus people between Fresno and Merced. Then, travelers will get back on the train if they're heading to further locations. Firefighters didn't attack the fire, they let the bridge actually burn. Fighting it would have been too dangerous in the riverbed and the bridge could have collapsed. **The fire is expected to be out around 2:00 p.m. Tuesday afternoon, and then Burlington Northern Santa Fe will have the tough task of getting the rail line back up and running.** Burlington Northern say the rail line should be back up and functional in 24 to 36 hours.
Source: http://abclocal.go.com/kfsn/news/111903_nw_rail_fire.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

11. *November 19, Herald Sun (Australia)* — **Crop sabotage. A militant animal rights group claims to have sabotaged the feed of a shipment of sheep bound for the Middle East from Australia, and say they will distribute video evidence of the action.** Patty Mark, a spokeperson for Animal Liberation, told Sky News this afternoon proof would be distributed to the media after police said they doubted the activists had managed to contaminate the food. Police say they have no evidence to back up the protesters' claims, made this morning, that pig meat was dumped into the food and water supply of the sheep, due to be loaded for transport tomorrow. The contamination was intended to stop the shipment being acceptable in its destination market, as Muslims do not eat pig meat. **The group is threatening to use the same tactics across Australia if the live export trade is not stopped.** A police spokesperson said officers at the scene said it was "very unlikely that the sheep were given anything but their regular food", and the owner of the sheep said the animals were vegetarian in any case.
Source: http://www.heraldsun.news.com.au/common/story_page/0,5478,79 14233%255E662,00.html

12. *November 19, Yahoo News* — **Brazilian growers prepare to fight Asian soy rust.** Soybean producers across Brazil have armed themselves this season in a battle against Asian soy rust. Brazil is set to become the world's No. 1 exporter of soy in 2003, displacing the United States from the top slot. **Experts agree that Brazil's future leadership in soy production will depend on how well it contains Asian rust, which is seen as the most destructive soybean leaf disease and can reduce yields by up to 80 percent.** Rust first showed up in Paraguay in 2001 and has since spread through Paraguay, Brazil, Bolivia, and parts of Argentina. U.S. producers are worried about the possibility of the fungus reaching U.S. soy fields. **Last season Asian soy rust hit Mato Grosso the hardest of the main soy states because growers there were caught off guard, unconvinced it could travel so fast across Brazil's massive 20 million hectare soy belt. Rust showed up late in the growing cycle last season but still managed to take three million tons off the 2002/03 crop, lowering Brazil's output to 52 million tons.** As Brazil enters the peak of a new planting season, Mato Grosso has already registered its first outbreaks of rust. **For now, producers are betting on a tough spraying campaign to hold off the scourge.**
Source: http://www.agprofessional.com/show_story.php?id=22352

[Return to top]

Food Sector

13. *November 18, Food Safety Inspection Service* — **Salad with turkey and ham recalled. LSG Sky Chefs, an Orlando, FL, establishment, is voluntarily recalling approximately 1,135 pounds of turkey and ham used in chef salads that may be contaminated with Salmonella, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday.** The salads were produced on November 11 and 12, 2003 and were distributed to retail stores in Florida. The problem was discovered through routine FSIS microbiological sampling. Consumption of food contaminated with Salmonella can cause salmonellosis, one of the most common bacterial foodborne illnesses. FSIS has received no reports of illness associated with consumption of this product.
Source: http://www.fsis.usda.gov/OA/recalls/prelease/pr059–2003.htm

14. *November 18, Food Safety Inspection Service* — **Roast beef recalled. The Butcher Block, an Indianola, NE, firm is voluntarily recalling approximately 110 pounds of cooked roast beef that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday.** The roast beef was produced and packaged on November 7 and distributed for use at a banquet in Indianola, NE, on November 9. FSIS has received no reports of illnesses associated with consumption of this product. The problem was discovered through routine FSIS microbiological testing. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/OA/recalls/prelease/pr058–2003.htm

[Return to top]

Water Sector

Nothing to report.

[]

Public Health Sector

15. *November 19, China Post* — **Suspected SARS case. A Kaohsiung hospital Tuesday reported this winter's first Severe Acute Respiratory Syndrome (SARS) case in Taiwan. Doctors at the Union Hospital said they diagnosed a resident of the southern Taiwan port city as a suspected SARS case.** The resident, whose identity was withheld, visited the hospital in the afternoon. He showed a typical SARS symptom of a high fever, doctors said. "He suffered from a fever for two days before coming to us," one doctor pointed out. The Kaohsiung resident returned from a trip to China not long ago. After the diagnosis, the patient was assigned to a pediatric ward.
Source: http://www.chinapost.com.tw/taiwan/detail.asp?ID=43300&GRP=B

16. *November 19, New York Times* — **Test of an experimental Ebola vaccine begins.** The first test in humans of an experimental vaccine against the Ebola virus began Tuesday, government scientists said. **The vaccine, administered by injection, was designed to try to prevent outbreaks of the lethal hemorrhagic fever where it occurs naturally in Africa. It is also a bid to thwart any efforts to use the highly infectious virus as a bioterrorist agent.** As part of a standard three−stage process, the first phase involves testing the vaccine's safety. Scientists also plan to measure immune responses among volunteers receiving the shots. No effective treatment exists against the viral infection, which kills up to 90 percent of victims quickly from severe internal bleeding. Ebola was discovered in 1976 in the Republic of Congo, then Zaire. Researchers plan to test the vaccine on 27 people, ages 18 to 44. They are expected to receive three injections of either the experimental vaccine or a placebo at the National Institute of Allergy and Infectious Diseases over two months. They will then be monitored for a year.
Source: http://www.nytimes.com/2003/11/19/health/19EBOL.html

17. *November 19, Dartmouth Medical School* — **Biofilm antibiotic resistance may be susceptible to genetic approach.** Biofilms, clusters of bacteria that are resistant to antibiotics, may have a genetic chink in their armor that could be exploited to combat the infections they cause. A study led by Dartmouth Medical School (DMS) researchers used a genetic−based approach to begin to understand how biofilms can withstand antibacterial treatments. The results of the study provide an innovative model for the investigation of biofilms that may lead to the development of new methods to hamper their resilience. "We are beginning to get at some of the mechanisms that might be important to understanding the antibiotic resistance of biofilms, which is the first step in the long journey to developing a treatment," said George O'Toole, assistant professor of microbiology and immunology at DMS. **Biofilms can form on industrial equipment, medical implants, teeth, and internal organs, and are estimated to be involved in 65 percent of human bacterial infections, according to the Centers for Disease Control and Prevention. Conventional antibiotic therapy, usually effective against free−floating bacteria, is frequently ineffective once pathogens have formed biofilms. Biofilms are up to 1,000−times more resistant to antibiotics.**
Source: http://www.eurekalert.org/pub_releases/2003−11/dms−bar111703 .php

18. *November 18, Reuters* — **Better security necessary at U.S. labs.** The Department of Homeland Security (DHS) should establish strict security guidelines for all government–funded U.S. laboratories that conduct research on deadly viruses, bacteria, and chemical agents, U.S. Department of Agriculture (USDA) investigators said on Tuesday. **The USDA's Office of Inspector General said it found dozens of research labs, mostly located at public universities, that were vulnerable to theft because of lax security and incomplete record keeping.** "Without a standard minimum level of security, there is a potential that laboratories could experience unauthorized entries and that the loss or theft of high consequence pathogens could go undetected," the report said. **With several federal agencies providing grants to many of the same research labs, the report recommended that DHS create one set of security rules for institutions that handle high risk agents.** Between July and September 2002, USDA investigators visited 104 laboratories at 11 sites and found many lacking alarm systems and surveillance cameras. At one institution, a science lecturer had stored seven vials of an agent that can cause pneumonic plague, an airborne pathogen that can kill all infected people within 48 hours, in an unlocked freezer.
Source: http://www.alertnet.org/thenews/newsdesk/N18164143.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

19. *November 19, Sioux City Journal* — **Aircraft monitors BPI ammonia leak. A one–of–a–kind aircraft has provided its services in determining the scope of the ammonia release Monday from Beef Products Inc., in South Sioux City, IA.** Dr. Mark J. Thomas, on–scene coordinator for the Environmental Protection Agency's Emergency Response and Removal Superfund Division and a crew from Airborne Imaging Inc. of Midlothian, TX, have used the high–tech aircraft to scan the site to monitor the release of ammonia. "I can say with certainty that you don't have concentrations that are leaving this property that are going to cause problems for the neighbors," Thomas said. "Basically, we found very small quantities of ammonia coming off the scene –– definitely below any type of concern." **At about 11 a.m. Monday, an ammonia line leak occurred at the plant located at 360 164th St. in South Sioux City. The ammonia is used in refrigeration at the plant that produces lean beef trimmings. At about 6 p.m. Monday, the Aero Commander 680 twin–engine aircraft arrived and began using infrared scanning equipment to determine the extent and location of the plume of ammonia from the leak.**
Source: http://www.siouxcityjournal.com/articles/2003/11/19/news/loc al/6847f98eaed86d6886256de30015f69f.txt

20. *November 19, Firehouse.com* — **Emergency medical services: ambulance hazards targeted. A major overhaul is planned in the way ambulances are operated, designed and regulated to make them less dangerous to the medics and patients who ride in them, top industry**

officials say. Confronting a chronic problem for the first time, the ambulance industry is working on a comprehensive plan to cut down on the number of deaths and injuries that result from the more than 6,500 ambulance crashes every year. The initiative could result in new standards for how drivers are screened and trained, more reliable ways to protect people and equipment inside the patient compartment and new designs to make the vehicles more crashworthy and less likely to roll over. **A Detroit News two−day series in January outlined how ambulance occupants were exposed to unnecessary risk because of a lack of safety standards regulating the patient compartment, poor vehicle design and inadequate seat belt systems. The problems, coupled with poor driver training, poor judgment and fatigue, were contributing factors in some of the 6,500 ambulance crashes each year.** Although the National Highway Traffic Safety Administration is the federal agency that oversees vehicle safety, it has been reluctant to set standards for ambulances and doesn't require them to be crash−tested.
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=17&id=22059

[Return to top]

Information and Telecommunications Sector

21. *November 19, Government Computer News* — **Congress plans report cards on cybersecurity.** On the heels of Office of Management and Budget efforts over the past year to boost cybersecurity, lawmakers are set to weigh in on agency progress. **The House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census next month will issue a cybersecurity report card detailing agency progress in meeting the requirements of the Federal Information Security Management Act** (FISMA). The subcommittee has been working to focus the legislative and executive branches on the importance of cybersecurity with a variety of hearings over the past year. Subcommittee staff director Bob Dix, speaking Wednesday, November 19, at the Enterprise Architecture 2003 Conference in Washington D.C. said the subcommittee also plans to explore whether the federal procurement process can be used to improve software security. "If we use the purchasing power of the federal government to insist that developers provide more secure products, that will benefit all users in both the public and private sectors," he said.
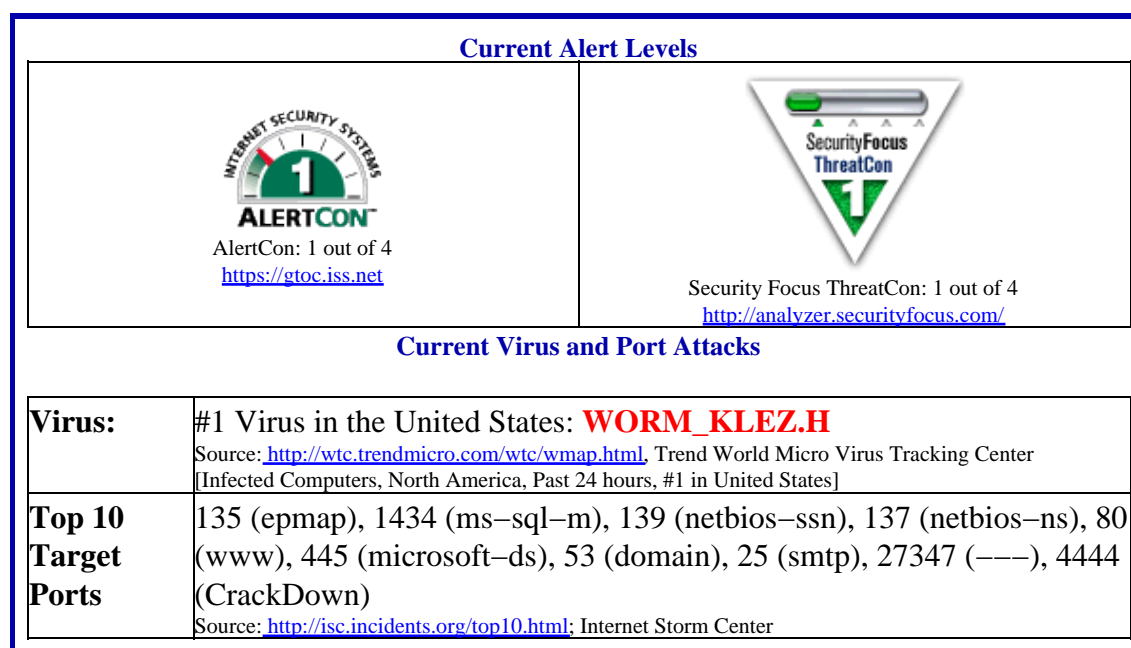Source: http://www.gcn.com/vol1_no1/daily−updates/24222−1.html

22. *November 19, Associated Press* — **UN: Scandinavia ahead in Internet access.** Scandinavia tops the world in access to the Internet and other communications technologies, the U.N. communications agency said Wednesday, November 19. **Sweden came in first in the Digital Access Index, followed by Denmark and Iceland, while Norway was fifth, said the International Telecommunications Union (ITU**). "Their presence at the top reflects that region's traditional emphasis on equitable access, affinity for technology and top−notch infrastructure," the ITU report said. South Korea, world leader in high−speed broadband access, came in fourth. **The United States was 11th, held back in part by its underdeveloped mobile phone system**, said Michael Minges, author of the report. The study measured 178 countries on a range of criteria, including the number of telephone lines and mobile phones per inhabitant, the cost of going online, national literacy, the speed of connections available and the percentage of inhabitants who are Internet users. **The study compared the top 40 countries in**

2002 with separate data it collected that showed the situation in 1998 to see how much change there had been. The index was prepared for leaders meeting next month in Geneva to discuss the possibility of making Internet access available to everyone on the planet. The report is available online:
http://www.itu.int/newsroom/press−releases/2003/30.html
Source: http://www.washingtonpost.com/wp−dyn/articles/A62434−2003Nov 19.html

Internet Alert Dashboard

Current Alert Levels	
AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: **WORM_KLEZ.H** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 139 (netbios−ssn), 137 (netbios−ns), 80 (www), 445 (microsoft−ds), 53 (domain), 25 (smtp), 27347 (−−−), 4444 (CrackDown) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

23. *November 19, Associated Press* — **Man fires on tourists on Israeli border.** A gunman trying to infiltrate an Israeli border crossing from Jordan fired on a crowd of tourists Wednesday, November 19, wounding five Ecuadoreans, officials said. **The shooting occurred at the Rabin terminal, an open−air checkpoint near Eilat, a Red Sea tourist town on Israel's southern tip, next to the Jordanian resort of Aqaba**. The military said the attacker leapt from the back of a truck and fired on a crowd before he was shot dead by security personnel. Nobody claimed responsibility, and Jordanian officials condemned the incident. **Jordanian government spokeswoman Asma Khader said the gunman was a Jordanian truck driver from Zarqa−−a predominantly Palestinian city**. The violence came as Egyptian mediators and the Palestinian prime minister traveled to the Gaza Strip on Wednesday to try to persuade militants to halt attacks on Israel, while Israel signaled willingness to scale back military operations in Gaza and the West Bank. A truce would be key to restarting the frozen U.S.−backed ``road map'' peace plan, which envisions a Palestinian state by 2005. Talks stalled several months ago because of violence and Palestinian political turmoil.
Source: http://www.nytimes.com/aponline/international/AP−Israel−Pale stinians.html?hp

---

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP
 To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer
 The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.